AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

1   1.   (Currently Amended) A method for maintaining secure network connections, the method

2   comprising:

3   detecting a change of address from an old address to a new address associated with a first

4   network element;

5   updating at least one first security configuration at the first network element;

6   transmitting at least one secure message from the first network element to a second

7   network element, wherein the at least one secure message comprises information associated with

8   the change of address; and contains both the old address and the new address,

9   updating wherein the old address and the new address in the at least one secure message

10   enables at least one second security configuration at the second network element based at least in

11   part on the at least one secure message to be updated.

1   2.   (Original) The method according to claim 1, wherein a lookup of security associations is

2   not dependent on any destination address.

1   3.   (Original) The method according to claim 1, wherein the first network element is a

2   mobile client and the second network element is a security gateway.

1   4.   (Original) The method according to claim 1, wherein the first network element and the

2   second network element are part of a virtual private network (VPN).

1   5.   (Original) The method according to claim 1, wherein communications between the first

2   network element and the second network element are based on a security architecture for the

3   internet protocol (IPsec).

1   6.   (Original) The method according to claim 5, wherein at least part of the communications

2   between the first network element and the second network element are based on an internet

3   security association and key management protocol (ISAKMP).

2

1   7.   (Currently Amended) The method according to claim 6, ~~wherein~~ further comprising the
2   second network element ~~identifies~~ identifying at least one security association based on at least
3   one cookie field in the at least one secure message.

1   8.   (Cancelled)

1   9.   (Currently Amended) At least one processor readable ~~carrier~~ medium for storing a
2   computer program of instructions configured to be readable by at least one processor for
3   instructing the at least one processor to execute a computer process for performing the method as
4   recited in claim 1.

1   10.   (Currently Amended) A method for maintaining secure network connections, the method
2   comprising:
3   duplicating, ~~between a second network element and~~ at a third network element,
4   information associated with a secure network connection between a first network element and
5   [[the]] a second network element, wherein a lookup of security associations associated with the
6   secure network connection is not dependent on any destination address; and
7   in response to detecting failure of the second network element, replacing the second
8   network element with the third network element in the secure network connection with the first
9   network element.

1   11.   (Currently Amended) The method according to claim 10 further comprising sending at
2   least one secure message from the third network element to the first network element to notify
3   the first network element that the secure network connection will be taken over by the third
4   network element.

3

1   12.   (Original) A method for maintaining secure network connections, the method
2   comprising:
3   configuring a plurality of security gateways such that a lookup of security associations is
4   not dependent on any destination address; and
5   sharing at least one security association among the plurality of security gateways.

1   13.   (Cancelled)

1   14.   (Currently Amended) The ~~system~~ first security server according to claim [[13]] 22,
2   wherein a lookup of security associations is not dependent on any destination address.

1   15. – 16. (Cancelled)

1   17.   (Currently Amended) The ~~system~~ first security server according to claim [[13]] 22,
2   wherein communications between the ~~first network element~~ mobile client and the ~~second~~
3   ~~network element~~ first security server are based on a security architecture for the internet protocol
4   (IPsec).

1   18. – 19. (Cancelled)

1   20.   (New) The method of claim 10, further comprising:
2   during life of the secure network connection between the first and second network
3   elements, the third network element receiving information relating to one or more security
4   associations of the secure network connection from the second network element.

1   21.   (New) The method of claim 20, wherein the first network element is a mobile client, and
2   the second and third network elements are security servers.

4

1   22.   (New) A first security server comprising:

2   a transceiver to receive information relating to at least one security association of a secure

3   network connection between a mobile client and a second security server; and

4   a processor module to:

5   monitor operation of the second security server;

6   in response to detecting failure of the second security server, send a message to

7   the mobile client that the first security server is taking over the secure network connection; and

8   communicate with the mobile client using the at least one security association

9   over the secure network connection between the first security server and the mobile client.

5